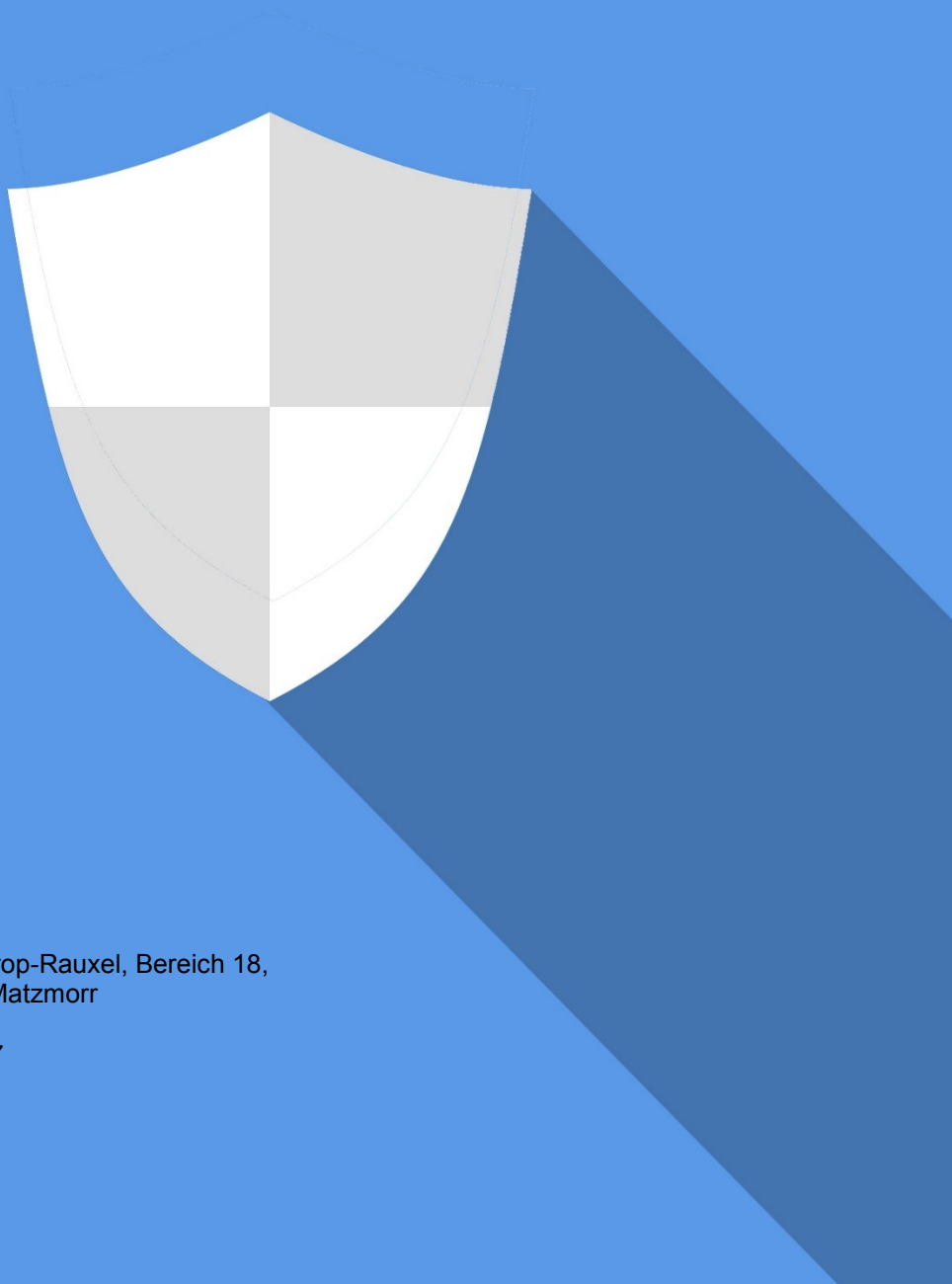
Leitlinie Informationssicherheit Stadt Castrop-Rauxel



erstellt von	Stadt Castrop-Rauxel, Bereich 18, Benjamin Matzmorr
Schutzklasse	öffentlich
Version	2020-08-17

Version	Datum	Autor	Kommentare
2019.12.000	18.12.2019	Peter Severidt	Entwurf
2020.01.001	23.01.2020	M. Großbröhmer	Anmerkungen aus Gladbeck
2020.01.002	27.01.2020	Peter Severidt	Kommentare zur Version 2020.01.001
2020.01.003	30.01.2020	Peter Severidt	Einarbeitung der Ergebnisse aus der Sitzung des AK IT-Strategie vom 30.01.2020
2020.02.001	11.02.2020	Peter Severidt	Anpassung des Entwurfes der Leitlinie
2020.02.002	20.02.2020	Peter Severidt	Einarbeitung der Ergebnisse aus der Sitzung des AK IT-Strategie vom 20.02.2020
2020.02.003	21.02.2020	Peter Severidt	Finale Version
2020-06-08	08.06.2020	Benjamin Matzmorr	Anpassungen Castrop-Rauxel
2020-06-16	16.06.2020	Benjamin Matzmorr	Anpassungen Pkt. 1.3
2020-08-17	17.08.2020	Benjamin Matzmorr	Finalisieren nach Abstimmung EUV, DSB, BM
2020-08-17	24.08.2020	Benjamin Matzmorr	VK Beschluss der Leitlinie am 24.08.2020

Inhalt

Abbildungsverzeichnis

1 Allgemeines

1.1 Hintergrund

Kommunalverwaltungen sind verpflichtet, ihre IT-Systeme und Verwaltungsvorgänge durch technische, physische und organisatorische Maßnahmen ausreichend abzusichern.

Diese Verpflichtungen ergeben sich u. a. aus:

- DSGVO - Datenschutz-Grundverordnung, Art. 32, Sicherheit der Verarbeitung
- GoBD - Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
- dem Grundsatz des rechtmäßigen Verwaltungshandelns (Rechtsstaatsprinzip Art. 20 Abs. 3 Grundgesetz)

Darüber hinaus sind hohe materielle und immaterielle Schäden (z. B. Rufschäden bzw. Vertrauensverlust) abzuwenden, die der Stadt Castrop-Rauxel durch den Bruch der Vertraulichkeit und durch Datenmanipulation (Verlust der Integrität) von Informationen oder durch Nichtverfügbarkeit der IT-Systeme und Anwendungen entstehen können.

Weiterhin sind die erheblichen Investitionen und Aufwände der Stadt Castrop-Rauxel über angemessene Sicherheitsvorkehrungen zu schützen.

1.2 Zweck

Die Leitlinie bildet und schafft die Grundlage für die Einführung, den Aufbau, die kontinuierliche Weiterentwicklung sowie die Verbesserung eines Informationssicherheitsmanagements, um

- dem Schutzbedarf der Informationen und dem Stand der Technik entsprechende technische, physische und organisatorische Maßnahmen zu ergreifen,
- die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen sicherzustellen,
- den Schutz der Daten in angemessenem Maße zu gewährleisten.

1.3 Geltungsbereich

Die Leitlinie für Informationssicherheit gilt für alle Organisationseinheiten der Stadtverwaltung Castrop-Rauxel. Die Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Bediensteten der Stadtverwaltung Castrop-Rauxel zu beachten und einzuhalten.

Die Leitlinie wird mit Hilfe der Sicherheitsorganisation und der Sicherheitsprozesse der Stadt Castrop-Rauxel umgesetzt und ausgestaltet.

Soweit Dritte als Auftragnehmer für die Stadt Castrop-Rauxel tätig sind, ist bei Auftragserteilung die Einhaltung der notwendigen Schutzmaßnahmen vertraglich zu regeln und zu kontrollieren.

Darüber hinaus gilt die Richtlinie (ausgenommen Punkt 5) analog auch für ihre verbundenen Unternehmen.

2 Informationssicherheitsziele und Schutzmaßnahmen

2.1 Informationssicherheitsziele

Die Ziele der Informationssicherheit sind:

- die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit
- der Schutz von Informationen, IT-Systemen, Anwendungen, Verfahren und Prozessen

um einen kontinuierlichen Verwaltungsbetrieb zu gewährleisten.

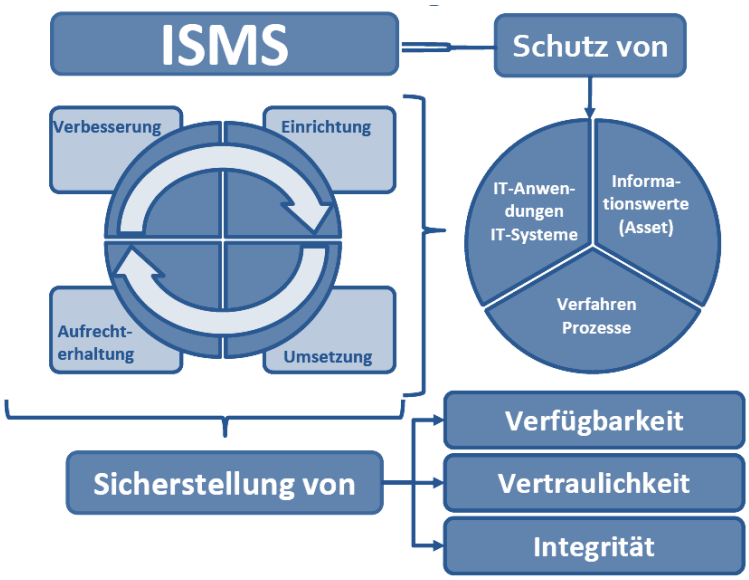


Abbildung 1: Informationssicherheitsziele

Um Beeinträchtigungen der Informationssicherheit zu minimieren, sind angemessene Schutzmaßnahmen erforderlich.

2.2 Schutzmaßnahmen

Die Schutzmaßnahmen umfassen:

- Organisatorische Vorkehrungen (verbindliche Regeln und Vorgaben)
- Technische Maßnahmen (Software, Hardware, Konfigurationen)
- Physische Sicherheit (Maßnahmen zur Vermeidung von Gefahren durch physische Einwirkungen auf die IT-Systeme)
- Personelle Maßnahmen (Schulungen, Mitarbeiterauswahl)

Die Schutzmaßnahmen orientieren sich mindestens an den Anforderungen der Basis-Absicherung des IT-Grundschutz-Kompendiums in der aktuellsten Edition [BSI-IT-GSK] und am *IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung [AG-MOD-IT-GS-2018]*.

Da insbesondere bei der Verarbeitung personenbezogener Daten in der Verwaltung der Schutzbedarf der Daten in der Regel nicht nur mit der Basis-Absicherung abgedeckt werden kann, ist eine Orientierung der Schutzmaßnahmen in diesen Fällen an den Anforderungen der Standard-Absicherung gemäß IT-Grundschutz-Kompendium in der aktuellsten Edition [BSI-IT-GSK] erforderlich.

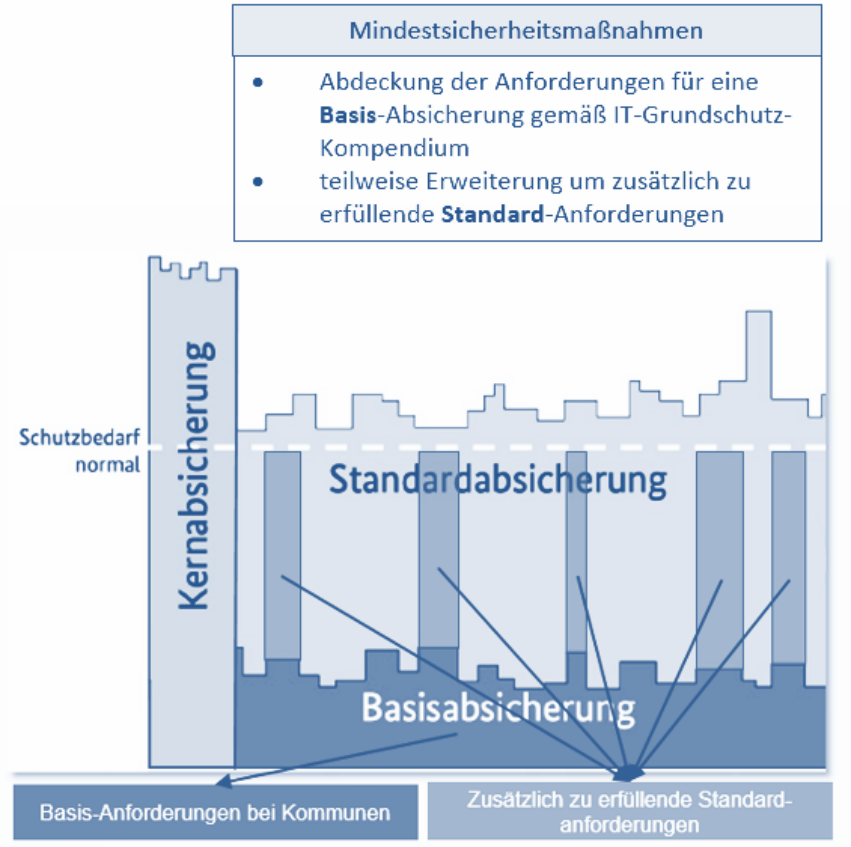


Abbildung 2: Mindestschutzmaßnahmen

3 Informationssicherheits-Managementsystem (ISMS)

Die Grundlage der Informationssicherheit der Stadt Castrop-Rauxel bildet der Aufbau und der Betrieb eines zentral koordinierten, bereichsübergreifenden Informationssicherheits-Managementsystems ISMS gemäß BSI-Standard 200-2 in der aktuellsten Fassung [BSI-200-2].

Zur Erreichung und Aufrechterhaltung eines angemessenen Sicherheits-Niveaus wird/werden

- Informationssicherheit zum integralen Bestandteil aller Geschäfts- und Arbeitsprozesse,
- die Informationssicherheit durch ein zentrales ISMS gesteuert und gelenkt,
- klare Verantwortlichkeiten sowie effektive Steuerungsinstrumente und Steuerungsprozesse etabliert,
- ausreichende finanzielle, personelle und zeitlichen Ressourcen bereitgestellt,
- Aufwand und Ziele in ein angemessenes Verhältnis zueinander gestellt,
- Wirtschaftlichkeit angestrebt.

4 Organisationsstruktur und Verantwortlichkeiten[1]

4.1 Bürgermeister der Stadt Castrop-Rauxel

Die Gesamtverantwortung für die Informationssicherheit liegt bei dem Bürgermeister der Stadt Castrop-Rauxel.

Der Bürgermeister ist insbesondere verantwortlich für die organisatorischen Vorkehrungen zur Umsetzung, Erhaltung und Weiterentwicklung der Informationssicherheit sowie für die technische, monetäre und personelle Ressourcen-Bereitstellung für die Informationssicherheit.

4.2 Informationssicherheitsbeauftragter (ISB)

Die Umsetzung der Informationssicherheitsprozesse bei der Stadt Castrop-Rauxel wird in Verantwortung eines (externen) Informationssicherheitsbeauftragten gesteuert.

Bei seiner Arbeit wird der (externe) Informationssicherheitsbeauftragte durch die Stadt Castrop-Rauxel unterstützt.

Der Informationssicherheitsbeauftragte baut das ISMS auf, setzt es um und entwickelt es weiter. Dabei sorgt er dafür, dass das ISMS in die relevanten Geschäftsprozesse eingebunden wird und kontrolliert die Wirksamkeit.

4.3 Führungskräfte

Die Führungskräfte (bzw. die Personalverantwortlichen) stellen sicher, dass die notwendigen organisatorischen, technischen, physischen und personellen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeitenden bzw. die in ihrem Verantwortungsbereich tätigen Nutzer durchgesetzt werden.

4.4 Mitarbeitende

Jeder Mitarbeitende trägt durch sein Verhalten zur Gewährleistung der Informationssicherheit bei. Alle Mitarbeitenden der Stadt Castrop-Rauxel sind sich ihrer Verantwortung für das Erreichen der Sicherheitsziele bewusst. Sie unterstützen diese Leitlinie und sind in den Informationssicherheitsprozess aktiv eingebunden.

Die Leitlinie der Informationssicherheit verpflichtet alle Mitarbeitenden dazu:

- vorgegebene Maßnahmen zum Schutz der verarbeiteten Daten hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität umzusetzen
- bei der Erfüllung der aus der Leitlinie resultierenden Anforderungen und Maßnahmen mitzuwirken
- sich aktiv am Aufbau und der kontinuierlichen Verbesserung des Informationssicherheits-Managements zu beteiligen
- Informationssicherheit als Qualitätsmerkmal und integraler Bestandteil zur Erfüllung ihrer Aufgaben in ihre Arbeitsprozesse zu integrieren
- das Erkennen vorhandener Bedrohungen gemäß dem definierten Meldeprozess unverzüglich zu melden und das Entwickeln angemessener Sicherheits- und Gegenmaßnahmen zu unterstützen
- die Bildungsangebote des Arbeitgebers zum Thema Informationssicherheit anzunehmen.

[1] Details hierzu sind der RL Informationssicherheitsorganisation zu entnehmen.

5 Zusammenarbeit im Zweckverband Gemeinsame Kommunale Datenzentrale Recklinghausen (GKD)

Vorhandene Prozessumsetzungen werden zwischen der GKD und ihren Mitgliedern ausgetauscht, um im Rahmen der interkommunalen Zusammenarbeit Synergieeffekte zu nutzen. Langfristig wird eine möglichst einheitliche Umsetzung angestrebt.

Die Funktion des externen ISB (siehe Ziffer 4.2) wird durch Dienstkräfte der GKD wahrgenommen.

6 Schulungs- und Sensibilisierungsmaßnahmen

Der Bürgermeister sowie die Personalverantwortlichen stellen sicher, dass Mitarbeitende mit den Zielen der Informationssicherheit vertraut sind.

Um einen angemessenen Umgang mit sensiblen Informationen zu gewährleisten, werden die Mitarbeitenden hierzu regelmäßig bzw. bei Bedarf im richtigen Umgang mit Sicherheitsaspekten unterrichtet.

7 Kontinuierlicher Verbesserungsprozess (KVP)

Zur Sicherstellung des angestrebten Informationssicherheitsniveaus werden interne Audits und eine kontinuierliche Überprüfung der getroffenen Regelungen vorgenommen.

Werden Abweichungen festgestellt, müssen Maßnahmen zur Verbesserung der Sicherheitssituation und zur Anhebung des Sicherheitsniveaus getroffen und umgesetzt werden.

Da die Informationssicherheit ein sich schnell entwickelndes Feld ist, wird diese Leitlinie in regelmäßigen Abständen auf ihre Aktualität und Wirksamkeit überprüft und gegebenenfalls angepasst.

8 Referenzen

[BSI-IT-GSK]	IT-Grundschutz-Kompendium; aktuellste Edition; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de
[AG-MOD-IT-GS-2018]	IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung; V1.0; 08.05.2018; ARBEITSGRUPPE „MODERNISIERUNG IT-GRUNDSCHUTZ“ mit Unterstützung durch Deutscher Städtetag, Deutscher Landkreistag, Deutscher Städte- und Gemeindebund
[BSI-200-2]	BSI-Standard 200-2 - IT-Grundschutz-Methodik; aktuellste Fassung; Bundesamt für Sicherheit in der Informationstechnik; (https://www.bsi.bund.de/grundschutz)